



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,905	04/03/2002	David Jay Duffield	RCA 89865	1250

7590 11/27/2006

Joseph S Tripoli  
Thomson Multimedia Licensing Inc  
PO Box 5312  
Princeton, NJ 08543-5312

EXAMINER

ZAND, KAMBIZ

ART UNIT PAPER NUMBER

2132

DATE MAILED: 11/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/089,905

Applicant(s)

DUFFIELD ET AL.

Examiner

Kambiz Zand

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on RCE filed on 11/08/2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 5-15, and 17-22 is/are rejected.
- 7) ☒ Claim(s) 2-4 and 16 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.


**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 03 April 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
KAMBIZ ZAND  
PRIMARY EXAMINER

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. The text of those sections of Title 35, U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 5, 13, 17, 19 and 21 have been amended.
4. Claims 1-22 are pending.

### *Response to Arguments*

5. Applicant's arguments with respect to the independent claims have been considered but are moot in view of the new ground(s) of rejection. Although examiner have provided a reference below but the access based on a comparison to a protected data is well known in the art and the same case law further applies to the added limitation.
6. Applicant's arguments with respect to added limitations are however persuasive only in the light of claims 2, 6, 16, and 18. Therefore the rejection of claims 2-4, 6, 16 and 18 has been withdrawn (see allowability subject matters below).
7. **Examiner suggests concentration on page 2 of the specification where the improvement over prior art is the reduction of number of bits based on selection of resources utilizing a certificate authority in transmission**

**between the source and the receiver based on partial authentication of their respective id's (see the last paragraph of the background of the invention and the summary of the invention) or see allowability subject matters below.**

***Claim Rejections - 35 USC § 112***

***8. The following is a quotation of the second paragraph of 35 U.S.C. 112:***

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

- 9. Claims 5-12, 17 and 18** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

**In claims 5, 7 and 17**, the "substantially" phrases makes the claims indefinite and unclear in that neither means nor interrelationship of means are set forth in these claims in order to achieve the desired results expressed in the "substantially" phrases. It is a relative term where such phrase may differ from one entity to other. Examiner suggests deletion of the phrase "substantially" from the above claims.

**In claim 12**, the "intentionally" phrases makes the claims indefinite and unclear in that neither means nor interrelationship of means are set forth in these claims in order to achieve the desired results expressed in the "intentionally" phrases. It is a relative term where such phrase may differ from one entity to other. Examiner suggests deletion of the phrase "intentionally" from the above claims.

10. Claims 6, 8-12 and 18 are rejected based on their dependency on the rejected claims above.

***Claim Rejections - 35 USC § 103***

11. **Claims 1, 5, 7-12, 13-15, 17 and 19-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Graunke (6,731,758 B1) in view of Epstein (6,490,355 B1).

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

**As per claims 1 and 21** teach a method for verifying that a source device that is capable of receiving protected content is authorized to communicate the protected content to a sink device that is capable of descrambling the protected content comprising:

receiving at said source device an approval code associated with said source and sink devices; determining, in said source device, a local code using data associated with said source and sink devices (see fig. 2, item, 208 and 209 sent from video sink device 104 to video source 102 and associated text); and

comparing, in said source device, at least a portion of said approval code to at least a portion of said local code (210 in fig.2 and associated text), and verifying that the sink device is authorized to receive the protected content from said source device in response to the comparison (see col.3, lines 6-22 and 51-56) but do not explicitly

Art Unit: 2132

disclose providing access to the protected content to the sink device based on the verification step above. However Epstein (6,490,355 B1) disclose providing access to the protected content to the sink device based on the verification step above (see fig.2-4 and associated texts).

It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize access method and system of Epstein in Graunke's ciphering/deciphering protection content in order to have proper access to the protected content (see col.7, lines 46-53).

**As per claim 14** teach the method according to claim 2, wherein said data associated with said source device for determining said local code is not public information and wherein said data associated with said sink device for determining said local code is public information (see Ak and Bk which corresponds to device identifier of the applicant).

**As per claims 5 and 17** teach a method for verifying that a source device that is capable of receiving protected content is authorized to communicate protected content to a sink device that is capable of descrambling the protected content comprising: providing unique identifiers associated with said source and sink devices to a validation authority; receiving from said validation authority an approval code, said approval code using data corresponding to said identifiers; determining, in said source device, a local code using said data associated

Art Unit: 2132

with said source and sink devices, and comparing at least a portion of said approval code to at least a portion of said local code. and verifying that the sink device is authorized to receive the protected content from the source device in response to the comparison (see as applied to claim 1 above; also col.3, lines 1-5, it also disclose unique device identifier Ak and Bk) but do not explicitly disclose providing access to the protected content to the sink device based on the verification step above. However Epstein (6,490,355 B1) disclose providing access to the protected content to the sink device based on the verification step above (see fig.2-4 and associated texts).

It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize access method and system of Epstein in Graunke's ciphering/deciphering protection content in order to have proper access to the protected content (see col.7, lines 46-53).

**As per claim 7** teach the method of Claim 5, wherein said identifiers are provided to said validation authority by said user (see the source and sink devices 102, 104 have been provided with an array of private keys and a complementary identifier by a certification authority).

**As per claims 8 and 22** teach the method of Claim 5, wherein said source device is selected from one of an access device and a media player and wherein said sink device is a digital television (see fig.4 and associated text).

Art Unit: 2132

**As per claim 9** teach the method of Claim 5, wherein said data associated with said source device is secured so as not to be readily ascertainable by said user.

**As per claim 12** teach the method of Claim 1, further comprising said source device communicating whether said source device is authorized to provide said content to said sink device to a user, and intentionally delaying communicating whether or not said compared approval code and local code are consistent (see 102 and 104 authorized devices as applied to claims above where they both possess and share a common secret authentication key  $K_m$ , and if authentication fails the communication is delayed).

**As per claim 13** teach the method for verifying that a selected device is authorized to receive protected content and for selecting at least one security key and at least one identifier used to access protected content, said method comprising:

receiving at a first device a plurality of security keys associated with said content;

receiving said identifier at said first device to be used to provide said content to a second device, said identifier being associated with said second device;

comparing said identifier with said plurality of security keys and verifying that said second device is authorized to receive said protected content in response to the

comparison, and selecting one of said plurality of security keys associated with said identifier using said first device; and,

providing said content to said second device using said first device and selected

security key (see fig.2. FIG. 2 illustrates a process based method for providing video



content from a source device to a sink device. Source and sink devices 102 and 104 are assumed to have each been provided with an array of private keys and a complementary identifier by a certification authority. As illustrated, upon power on or reset, source device 102 first provides a basis value to the symmetric ciphering/deciphering process to sink device 104 (block 202). For the illustrated embodiment, the basis value is a random number ( $A_n$ ).  $A_n$  may be generated in any one of a number of techniques known in the art. Additionally, source device 102 also provides its identifier ( $A_k$ ) to sink device 104 (block 202). In response, sink device 104 replies with its identifier ( $B_k$ ) (block 203). Upon exchanging the above information, source and sink devices 102 and 104 independently generate their respective copies of an authentication key ( $K_m$ ) using  $A_k$  and  $B_k$  (block 204 and 205). For the illustrated embodiment, source device 102 generates its copy of  $K_m$  by summing private keys of its provided array indexed by  $B_k$ , while sink device 104 generates its copy of  $K_m$  by summing private keys of its provided array indexed by  $A_k$ . At this time, if both source and sink devices 102 and 104 are authorized devices, they both possess and share a common secret authentication key ( $K_m$ ) but do not explicitly disclose providing access to the protected content to the sink device based on the verification step above. However Epstein (6,490,355 B1) disclose providing access to the protected content to the sink device based on the verification step above (see fig.2-4 and associated texts).

It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize access method and system of Epstein in Graunke's

Art Unit: 2132

ciphering/deciphering protection content in order to have proper access to the protected content (see col.7, lines 46-53).

**As per claims 15, 19 and 20** teach a method for verifying that a set top box is authorized to communicate protected content to a digital television comprising: receiving at said set top box an approval code associated with said set top box and said digital television; determining, in said set top box, a local code using data associated with said set top box and said digital television; and comparing at least a portion of said approval code to at least a portion of said local code, and verifying that said digital television is authorized to receive said protected content from said set top box in response to the comparison; wherein the approval code is generated using the respective serial numbers of the set top box and the digital television. (see as applied to claim 1 above in addition to item 108A in fig.4 deals with set up box) but do not explicitly disclose providing access to the protected content to the sink device based on the verification step above. However Epstein (6,490,355 B1) disclose providing access to the protected content to the sink device based on the verification step above (see fig.2-4 and associated texts).

It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize access method and system of Epstein in Graunke's ciphering/deciphering protection content in order to have proper access to the protected content (see col.7, lines 46-53).

**As per claim 10** teach all limitation of the claim as applied to claims above including certification authority but do not explicitly disclose usage of "public key". However usage of the public key by certificate authority is well known method as Graunke have refer to it indirectly by using the "private keys" which are usually paired with the public keys in order to transmit a common secret between the two entities.

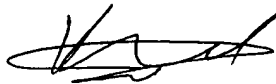
**As per claim 11** Graunke (6,731,758 B1) teach the method according to claim 10, wherein said data associated with said source device for determining said local code is not public information and wherein said data associated with said sink device for determining said local code is public information (see Ak and Bk which corresponds to device identifier of the applicant).

***Allowable Subject Matter***

12. **Claims 2-4 and 16** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.
13. **Claims 6, and 18** would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

### Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Please see enclosed PTO-892.
15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are 571-272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



KAMBIZ ZAND  
PRIMARY EXAMINER

11/24/2006

AU 2132